明　細　書

# 情報処理装置および情報処理装置におけるセキュリティ確保方法

## 技　術　分　野

本発明は、情報処理装置および情報処理装置におけるセキュリティ確保方法に関し、特に、１台の情報処理装置を複数のユーザが共有する場合に、個々のユーザが作成したデータのセキュリティを確保する技術に関する。

## 背　景　技　術

パソコンなどの情報処理装置は、複数のユーザによって共有されることが少なくない。このため、パソコンなどの情報処理装置用のオペレーションシステム（以下、単にＯＳという）も、複数ユーザによって共有されることを前提とした機能を備えている。たとえば、ＵＮＩＸ、ＷｉｎｄｏｗｓＸＰ（登録商標）、ＭａｃＯＳＸ（登録商標）などの最近の代表的なＯＳでは、個々のユーザがシステムの利用開始時にログオン手続（ＯＳによってはログイン手続と呼ばれている）を行い、利用終了時にログオフ手続（ＯＳによってはログアウト手続と呼ばれている）を行うのが基本的な利用形態となっている。

このように複数のユーザが同一の情報処理装置を共有する環境下では、個々のユーザが作成したデータに関して、十分なセキュリティが確保されるような配慮が重要である。たとえば、第１のユーザが作成したデータファイルに対して、第２のユーザが無制限に読み書き可能であるとすると、他人には閲覧させたくないファイルや他人には改変されたくないファイルを、共有環境下にある情報処理装置で取り扱うことはできなくなる。

そこで、共有環境下にある情報処理装置においても、個々のユーザごとのセキュリティを確保するために、同時に複数のユーザによる重複ログオンが行わ

れることがないような仕組みを採用し、個々のユーザごとにそれぞれ固有のアクセス権限を付与するような運用が行われている。たとえば、特開２００３－２８０７８１号公報には、個々のユーザごとに異なるアクセス権限を設定しておき、ログオン中のユーザが切り替えられたときに、アクセス権限も切り替えるための手法が開示されている。

上述したように、同一の情報処理装置を複数のユーザで共有する場合、個々のユーザごとに固有のアクセス権を設定しておき、所定のアカウントおよびパスワードを用いてログオンしたユーザに対して、当該ユーザに設定されたアクセス権の範囲内でデータファイルへのアクセスを許可する方法が、多くのＯＳにおいて採用されている。しかしながら、このような方法では、必ずしも十分なセキュリティを確保することはできない。たとえば、多くのＯＳでは、管理者権限をもった特別なユーザ（たとえば、ＵＮＩＸにおけるsuper user）の存在が認められており、この特別なユーザとしてログインすれば、何ら制限を受けることなく、すべてのデータファイルにアクセスすることが可能になる。また、情報処理装置内にデータファイルが格納されている以上、不正な方法を用いれば、いかなるデータに対してもアクセスすることが可能になる。

そこで本発明は、同一の情報処理装置を複数のユーザで共有する場合、個々のユーザが作成したデータについて、より十分なセキュリティを確保することが可能な方法を提供することを目的とする。

## 発　明　の　開　示

(1)　本発明の第１の態様は、情報処理装置において、

データファイルを格納するためのデータ格納部と、

このデータ格納部に格納されているデータファイルを必要に応じて展開するためのメモリと、

複数のユーザによる重複ログオンが行われることがないように、所定のユー

ザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部と、

ログオン中のユーザの操作に基づいて、データ格納部に格納されている所定のデータファイルをメモリ上に展開するファイル展開処理と、メモリ上に展開されている所定のデータファイルをデータ格納部に格納するファイル保存処理と、を実行する展開保存部と、

ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、メモリ上に新たなデータファイルを作成する処理もしくはメモリ上に展開されている既存のデータファイルに対する更新処理を実行するプログラム実行部と、

特定のユーザがログオフ手続を実行したときに、データ格納部に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、退避対象ファイルをネットワークを介して外部の記憶装置にコピーすることにより退避させる退避処理と、データ格納部内に格納されている退避対象ファイルを削除する削除処理と、外部の記憶装置に退避された退避対象ファイルをデータ格納部内にコピーして復元するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所に保存する管理情報保存処理と、を実行する退避処理部と、

上記特定のユーザがログオン手続を実行した後、必要に応じて、管理情報を参照することにより、外部の記憶装置に退避されている退避対象ファイルをデータ格納部内にコピーして復元する復元処理を実行する復元処理部と、

を設けるようにしたものである。

(2) 本発明の第２の態様は、上述の第１の態様に係る情報処理装置において、

復元処理部が、データファイルの保存時の階層構造を復元する予備復元処理と、この予備復元処理によって復元された階層構造内から選択された特定のデ

ータファイルを復元する本復元処理と、を実行するようにしたものである。

(3) 本発明の第３の態様は、上述の第１または第２の態様に係る情報処理装置において、

退避処理部が、予め定められた退避対象フォルダ内に格納されているデータファイルを、退避対象ファイルとして認識するようにしたものである。

(4) 本発明の第４の態様は、上述の第１または第２の態様に係る情報処理装置において、

退避処理部が、予め定められた所定の拡張子がファイル名に付されているデータファイルを、退避対象ファイルとして認識するようにしたものである。

(5) 本発明の第５の態様は、上述の第１～第４の態様に係る情報処理装置において、

退避処理部が、管理情報保存処理を実行する際に、着脱自在な携帯可能情報記録媒体に管理情報を保存し、

復元処理部が、復元処理を実行する際に、この携帯可能情報記録媒体に保存されている管理情報を参照するようにしたものである。

(6) 本発明の第６の態様は、上述の第１～第５の態様に係る情報処理装置において、

管理情報として、退避対象ファイルの退避先となる外部の記憶装置のアドレス情報を用いるようにしたものである。

(7) 本発明の第７の態様は、上述の第１～第６の態様に係る情報処理装置において、

退避処理部が、退避処理を実行する際に、退避対象ファイルを所定の分割方法に基づいて複数の分割ファイルに分割し、個々の分割ファイルをそれぞれ異なる複数の記憶装置に退避させる処理を実行し、この所定の分割方法を示す情報を含む管理情報を作成するようにし、

復元処理部が、管理情報に含まれている分割方法を示す情報に基づいて、退

避対象ファイルの復元を行うようにしたものである。

(8) 本発明の第８の態様は、上述の第１～第７の態様に係る情報処理装置において、

退避処理部が、退避処理を実行する際に、退避対象ファイルを所定の暗号化方法に基づいて暗号化した上で外部の記憶装置に退避させる処理を実行し、この所定の暗号化方法を示す情報を含む管理情報を作成するようにし、

復元処理部が、管理情報に含まれている暗号化方法を示す情報に基づいて復号化処理を実行し、退避対象ファイルの復元を行うようにしたものである。

(9) 本発明の第９の態様は、上述の第１～第８の態様に係る情報処理装置において、

退避処理部が、削除処理を実行する際に、メモリに展開されている退避対象ファイルに対しても削除する処理を行うようにしたものである。

(10) 本発明の第１０の態様は、上述の第１～第９の態様に係る情報処理装置としてコンピュータを機能させるコンピュータプログラムを用意し、このプログラムをコンピュータ読取り可能な記録媒体に記録して配付できるようにしたものである。

(11) 本発明の第１１の態様は、

データファイルを格納するためのデータ格納部と、

このデータ格納部に格納されているデータファイルを必要に応じて展開するためのメモリと、

複数のユーザによる重複ログオンが行われることがないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部と、

ログオン中のユーザの操作に基づいて、データ格納部に格納されている所定のデータファイルをメモリ上に展開するファイル展開処理と、メモリ上に展開されている所定のデータファイルをデータ格納部に格納するファイル保存処理

と、を実行する展開保存部と、

ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、メモリ上に新たなデータファイルを作成する処理もしくはメモリ上に展開されている既存のデータファイルに対する更新処理を実行するプログラム実行部と、

を備える情報処理装置を、複数のユーザで共用する場合に、個々のユーザごとにデータのセキュリティを確保する方法において、

特定のユーザがログオフ手続を実行したときに、データ格納部に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、退避対象ファイルをネットワークを介して外部の記憶装置にコピーすることにより退避させる退避処理と、データ格納部内に格納されている退避対象ファイルを削除する削除処理と、外部の記憶装置に退避された退避対象ファイルをデータ格納部内にコピーして復元するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所に保存する管理情報保存処理と、を実行する退避処理段階と、

上記特定のユーザがログオン手続を実行した後、必要に応じて、管理情報を参照することにより、外部の記憶装置に退避されている退避対象ファイルをデータ格納部内にコピーして復元する復元処理を実行する復元処理段階と、

を情報処理装置に行わせるようにしたものである。

(12) 本発明の第１２の態様は、上述の第１１の態様に係る情報処理装置におけるセキュリティ確保方法において、

復元処理段階が、データファイルの保存時の階層構造を復元する予備復元段階と、この予備復元段階によって復元された階層構造内から選択された特定のデータファイルを復元する本復元段階と、によって構成されるようにしたものである。

(13) 本発明の第１３の態様は、上述の第１１または第１２の態様に係るセキュリティ確保方法における退避処理段階および復元処理段階をコンピュータに実行させるコンピュータプログラムを用意し、このプログラムをコンピュータ読取り可能な記録媒体に記録して配付できるようにしたものである。

本発明に係る情報処理装置および情報処理装置におけるセキュリティ確保方法によれば、個々のユーザがログオフする時点で、セキュリティ確保が必要な退避対象ファイルが外部の記憶装置へ退避され、データ格納部からは削除されてしまうため、退避対象ファイルは情報処理装置内には残らなくなる。したがって、当該情報処理装置が複数のユーザによって共有されていたとしても、十分なセキュリティを確保することが可能になる。

## 図面の簡単な説明

図１は、本発明の一実施形態に係る情報処理装置１００の運用状態を示すブロック図である。

図２は、図１に示す情報処理装置１００におけるデータ格納部１１０内に格納されたデータファイルの階層構造を示すウインドウ表示の一例を示す図である。

図３は、図１に示す情報処理装置１００に関するものであり、図(a) は退避処理前のデータ格納部１１０の状態を示す図、図(b) は退避処理後のデータ格納部１１０および外部の記憶装置３００の状態を示す図である。

図４は、図１に示す情報処理装置１００の復元処理部１７０による二段階の復元処理機能の概念を示す図である。

図５は、退避対象ファイルに対する分割処理の概念を示す図である。

図６は、退避対象ファイルに対する分割処理を行うために、ネットワーク２００に３つの異なる記憶装置を接続した変形例を示すブロック図である。

## 発明を実施するための最良の形態

以下、本発明を図示する実施形態に基づいて説明する。

＜＜＜　§１．情報処理装置の基本構成　＞＞＞

図１は、本発明の一実施形態に係る情報処理装置１００の運用状態を示すブロック図である。図１において、一点鎖線で囲った部分が本発明に係る情報処理装置１００である。図示のとおり、この情報処理装置１００は、データ格納部１１０、展開保存部１２０、メモリ１３０、ユーザ管理部１４０、プログラム実行部１５０、退避処理部１６０、復元処理部１７０によって構成されている。これらの各構成要素のうち、データ格納部１１０、展開保存部１２０、メモリ１３０、ユーザ管理部１４０、プログラム実行部１５０は、従来の一般的な情報処理装置１００に備わっている構成要素であり、退避処理部１６０および復元処理部１７０が、本発明に特有の構成要素になる。

情報処理装置１００は、いわゆるコンピュータによって構成される装置であり、ここでは、特に、汎用のパソコンによって情報処理装置１００を構成した例を述べることにする。データ格納部１１０は、データファイルを格納するための構成要素であり、パソコンの場合、内蔵もしくは外付けのハードディスク装置によって構成されるのが一般的である。もちろん、光磁気ディスク装置や書換え可能な光ディスク装置（ＣＤ－ＲＡＭ装置など）によってデータ格納部１１０を構成することも可能である。一方、メモリ１３０は、データ格納部１１０に格納されているデータファイルを必要に応じて展開するための構成要素であり、通常、ＲＡＭによって構成される。

データ格納部１１０がデータファイルの格納場所として機能するのに対し、メモリ１３０はデータファイルに対する作業場所として機能する。展開保存部１２０は、必要に応じて、データ格納部１１０に格納されている所定のデータファイルをメモリ１３０上に展開するファイル展開処理と、メモリ１３０上に展開されている所定のデータファイルをデータ格納部１１０に格納するファイ

ル保存処理と、を実行する構成要素である。パソコンを情報処理装置１００として用いた場合、展開保存部１２０は、ＯＳプログラムの機能の一部として実現されることになる。

ユーザが、アプリケーションプログラムによって、データ格納部１１０内のデータファイルに対して所定の処理作業を実行する際には、まず、展開保存部１２０のファイル展開処理によって、データ格納部１１０内の作業対象となるデータファイルが、メモリ１３０上に展開される。この作業は、通常、アプリケーションプログラムによって、作業対象となるデータファイルを開く処理として実行される。図１には、データ格納部１１０に格納されている３つのデータファイルＦ１～Ｆ３のうちのファイルＦ２を開く操作が行われた状態が示されている。データ格納部１１０内に格納されていたデータファイルＦ２は、メモリ１３０上に展開された状態となっている。

プログラム実行部１５０は、所定のアプリケーションプログラムを実行し、メモリ１３０上に展開されている既存のデータファイルに対する更新処理を実行する機能を有する。図示の例の場合、プログラム実行部１５０は、メモリ１３０上に展開されているデータファイルＦ２に対して所定の更新処理を実行することになる。データファイルＦ２に対して加えられる更新処理の内容は、アプリケーションプログラムの種類やユーザが実行する操作によって様々である。結局、プログラム実行部１５０は、所定のアプリケーションプログラムを格納する手段と、これを実行するための演算処理手段によって構成されることになる。

上述したとおり、メモリ１３０は、データファイルに対する作業場所として機能する構成要素であり、アプリケーションプログラムによる作業対象となるデータファイルを一時的に保持する役割しか果たさない。したがって、メモリ１３０上で所定の作業が完了したデータファイルは、再びデータ格納部１１０へと格納される。この作業は、通常、アプリケーションプログラムによって、

作業対象となるデータファイルを保存する処理として実行される。この場合、元のファイル名と同一のファイル名で保存すると、いわゆる上書き保存がなされ、別なファイル名で保存すると、新たなデータファイルとしての保存がなされる。たとえば、図示の例において、メモリ１３０上に展開されているデータファイルＦ２に対する作業が完了し、更新処理がなされた場合、これを「Ｆ２」なる同一のファイル名で保存すると、データ格納部１１０内のデータファイルＦ２は、メモリ１３０上の更新されたデータファイルＦ２に置き換えられることになるが（上書き保存）、たとえば、「Ｆ４」などの別なファイル名で保存すると、データ格納部１１０内に格納されていたデータファイルＦ２はそのままの状態で、新たに「Ｆ４」なるファイル名のデータファイルが追加される。

なお、プログラム実行部１５０は、所定のアプリケーションプログラムの実行により、メモリ１３０上に新たなデータファイルを作成する処理を行う機能も有している。この機能は、通常、アプリケーションプログラムによる新規ファイルの作成作業として実行される。こうしてメモリ１３０上に新規作成されたデータファイルは、最終的には、保存処理によって、データ格納部１１０内に保存されることになる。

結局、展開保存部１２０によるデータ展開処理やデータ保存処理、プログラム実行部１５０による所定のアプリケーションプログラムの実行処理は、いずれも情報処理装置１００に対するユーザの入力操作に基づいて行われるが、複数のユーザによる共用を前提とした情報処理装置１００の場合、個々のユーザはそれぞれ所定のログオン手続を行うことにより情報処理装置１００に対する作業を開始し、所定のログオフ手続を行うことにより情報処理装置１００に対する作業を終了することになる。ここで、「ログオン」とは、所定のユーザが所定のアカウント（ユーザ名）および必要に応じて所定のパスワードを入力して、情報処理装置１００に対する利用状態を確保することを言い、「ログオフ」とは、現在ログオン中のユーザの利用状態を終了させることを言う。なお、ＯＳによ

っては、「ログオン」の代わりに「ログイン」なる文言を用い、「ログオフ」の代わりに「ログアウト」なる文言を用いる場合もあるが、本明細書において両者は同義である。また、ＯＳによっては、ログオフ手続を行うことなしに、シャットダウン操作（ＯＳの機能を終了させ、電源を切る操作）が可能なものもあるが、本明細書にいうログオフ手続とは、このようなシャットダウン操作により利用状態を終了させる手順も含むものである。

ユーザ管理部１４０は、複数のユーザによる重複ログオンが行われることがないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理を行う構成要素である。最近のパソコン用ＯＳには、このユーザ管理部１４０の機能が、ＯＳプログラムの機能の一部として標準装備されている。

なお、この実施形態の場合、ユーザ管理部１４０は、重複ログオンが行われることがないようなユーザ管理を行うだけでなく、現在ログオン中のユーザに対するアクセス権の管理も行う機能を有している。すなわち、ユーザ管理部１４０は、予め複数のユーザについてのアクセス権限を登録する機能を有しており、現時点でログオンしているユーザが誰であるかを認識し、展開保存部１２０およびプログラム実行部１５０に対して、当該ユーザのアクセス権の範囲内での処理動作のみを許可する監督処理を行う。たとえば、他のユーザが作成したデータファイルに対する読み書きの権限が一切与えられていないユーザがログオンしている場合、他のユーザが作成したデータファイルを展開しようとする展開保存部１２０の処理動作はユーザ管理部１４０によって許可されないことになる。同様に、他のユーザが作成したデータファイルに対する読み出し権限は与えられているが、書き込みの権限が与えられていないユーザがログオンしている場合、他のユーザが作成したデータを改変しようとするプログラム実行部１５０の処理動作、あるいは、改変後のデータをデータ格納部１１０に上

書き保存する展開保存部１２０の処理動作は、ユーザ管理部１４０によって許可されないことになる。

以上、情報処理装置１００の構成要素のうち、データ格納部１１０～プログラム実行部１５０までの機能を説明したが、これら５つの構成要素の各機能は、いずれも最近のパソコン用ＯＳが標準的に備えている機能であり、これら５つの構成要素を備える情報処理装置１００は、最近のＯＳ（たとえば、ＷｉｎｄｏｗｓＸＰ（登録商標），ＭａｃＯＳＸ（登録商標）、ＵＮＩＸなど）を組み込んだ標準的なパソコンというべきものである。そして、この標準的なパソコンでは、ＯＳが、複数ユーザによる共用を前提として設計されているため、上述のように、利用を開始するユーザには、所定のユーザ名によるログオン手続が原則的には要求され、当該ユーザ名の下で設定されたアクセス権の範囲内で、個々のデータファイルへのアクセスが許可されることになる。

しかしながら、既に述べたとおり、このような方法では、必ずしも十分なセキュリティを確保することはできない。たとえば、ＵＮＩＸにおけるsuper userのような管理者権限をもった特別なユーザとしてログインすれば、何ら制限を受けることなく、すべてのデータファイルにアクセスすることが可能になる。また、データ格納部１１０内にデータファイルが格納されている以上、不正な方法を用いれば、いかなるデータファイルに対してもアクセスすることは可能である。

＜＜＜　§２．本発明の基本的な特徴　＞＞＞

本発明の目的は、§１で述べたように、同一の情報処理装置１００を複数のユーザで共有する場合、個々のユーザが作成したデータについて、より十分なセキュリティを確保することにある。そのため、本発明に係る情報処理装置１００には、退避処理部１６０および復元処理部１７０という本発明に固有の構成要素が付加されている。また、本発明を実施する上では、情報処理装置１００をネットワーク２００に接続し、このネットワーク２００に接続された外部

の記憶装置３００を利用できる環境が必要である。

もっとも、現在、パソコンなど情報処理装置１００は、ネットワーク２００に接続して利用するのが一般的になりつつあるので、多くの情報処理装置１００には、既にネットワーク２００への接続環境が整っていることになる。ネットワーク２００としては、社内ＬＡＮなどのローカルなネットワークを利用してもよいし、インターネットを利用してもかまわない。また、外部の記憶装置３００としては、このネットワーク２００を介してアクセス可能な記憶装置であれば、どのような装置を用いてもかまわない。一般的には、データサーバやバックアップサーバなどのサーバ装置を外部の記憶装置３００として用いると便利である。結局、パソコンなど、既存の情報処理装置１００の多くは、既に、ネットワーク２００を介して外部の記憶装置３００へアクセスする環境下にあるのが一般的であり、そのような情報処理装置１００については、既存の環境をそのまま利用して本発明の実施が可能である。

一方、本発明を実施する上では、情報処理装置１００外に管理情報を記憶させる記憶場所を用意しておく必要がある。図１に示す例では、携帯可能情報記録媒体４００を、この記憶場所として利用している。具体的には、この実施形態の場合、ＩＣカードを携帯可能情報記録媒体４００として用いている。ＩＣカードにアクセスを行う場合、通常、専用のリーダライタ装置が必要になるので、この実施形態では、情報処理装置１００として用いるパソコンに、リーダライタ装置を接続し、このリーダライタ装置にＩＣカードを挿入することにより、パソコンからのアクセスが可能になるようにしている。もちろん、ＩＣカードは、着脱自在な携帯可能情報記録媒体４００であり、随時、リーダライタ装置から抜き出して携帯することが可能である。

結局、本発明を実施するために、情報処理装置１００の内部に新たに設けた構成要素は、退避処理部１６０と復元処理部１７０ということになる。本発明の基本概念は、特定のユーザがログオフ手続を実行する際に、当該特定のユー

ザがデータ格納部１１０内に保存したデータファイルを、外部の記憶装置３００へと退避させ、データ格納部１１０内のデータファイルを削除してしまうことにある。退避処理部１６０は、この退避のための処理を実行する構成要素である。この退避処理により、当該ユーザが作成したデータファイルは、情報処理装置１００内から削除されて存在しなくなってしまうため、後に、別なユーザが同じ情報処理装置１００にログオンした場合でも、十分なセキュリティが確保できることになる。もちろん、当該特定のユーザが再度ログオンしたときには、外部の記憶装置３００に退避させていたデータファイルをデータ格納部１１０内へ復元する必要がある。復元処理部１７０は、この復元処理を行う構成要素である。以下、退避処理部１６０の機能および復元処理部１７０の機能を詳述する。

退避処理部１６０は、図１に示されているとおり、５つの処理機能を有している。いずれの処理も、現在ログオン中のユーザがログオフ手続を実行したときに実行されることになる。前述したとおり、ユーザのログオン手続およびログオフ手続は、ユーザ管理部１４０によって処理される。ユーザ管理部１４０は、現在ログオン中のユーザがログオフ手続を実行した場合、その旨を退避処理部１６０へ報告し、この５つの処理機能の実行を促すことになる。

退避処理部１６０で最初に実行される退避対象認識処理は、特定のユーザがログオフ手続を実行したときに、データ格納部１１０に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する処理である。たとえば、図示の例において、現在ログオン中のユーザを「ユーザ甲」と呼ぶことにし、このユーザ甲のログオン中の作業に基づいて、３つのデータファイルＦ１，Ｆ２，Ｆ３が作成もしくは更新されたものとしよう。この場合、図示のとおり、データ格納部１１０内には、３つのデータファイルＦ１，Ｆ２，Ｆ３が格納された状態になっている。ここで、ユーザ甲の作業に基

づいて作成もしくは更新されたデータファイルの全部を退避対象ファイルとして認識することにしておけば、図示の例の場合、ユーザ甲がログオフ手続を実行したとき、データ格納部１１０内に格納されている３つのデータファイルＦ１，Ｆ２，Ｆ３のすべてが、退避対象ファイルとして認識されることになる。

退避処理部１６０で実行される第２の処理は、この退避対象ファイルをネットワーク２００を介して外部の記憶装置３００にコピーすることにより退避させる退避処理である。上述の例の場合、データ格納部１１０内に格納されている３つのデータファイルＦ１，Ｆ２，Ｆ３のすべてが、退避対象ファイルとして認識されているので、この３つのデータファイルＦ１，Ｆ２，Ｆ３のすべてが、ネットワーク２００を介して外部の記憶装置３００へとコピーされることになる。このコピー処理自体は、いわばバックアップ処理と同等の作業になる。

退避処理部１６０で実行される第３の処理は、データ格納部１１０内に格納されている退避対象ファイルを削除する削除処理である。この削除処理を伴う点が、一般的なバックアップ処理と異なる点である。上述した退避処理により、退避対象ファイルＦ１，Ｆ２，Ｆ３が外部の記憶装置３００へコピーされたわけであるが、この削除処理により、コピー元となったデータ格納部１１０内のオリジナルの退避対象ファイルＦ１，Ｆ２，Ｆ３が削除されることになるので、結果的に、上述した退避処理は、バックアップとしての意味はもたないことになる。

なお、一般に、ハードディスク装置などのデータ格納部１１０に格納されているデータファイルを削除する方法として、当該データファイルをそのディレクトリ上において削除する方法（ディレクトリを書き換えることにより、ディレクトリ上は当該ファイルが存在していないこととする方法）と、実際のデータ記録領域に別なデータを上書きすることによりデータファイル自身を完全に削除する方法と、が知られているが、本発明を実施する上では、いずれの方法を採ってもかまわない。前者の方法よりも後者の方法の方が、より高いセキュ

リティを確保する上では好ましいが、削除処理の負担という点では、前者の方法の方が後者の方法よりも負担が軽くなる。

退避処理部１６０で実行される第４の処理は、外部の記憶装置３００に退避された退避対象ファイルを、将来、データ格納部１１０内にコピーして復元するために必要な管理情報を作成する管理情報作成処理である。ここで作成する管理情報は、外部の記憶装置３００に退避された退避対象ファイルをデータ格納部１１０内にコピーして復元することが可能な情報であれば、どのような形態の情報でもかまわないが、一般的には、退避対象ファイルの退避先となる外部の記憶装置３００のアドレス情報を管理情報として用いるようにすればよい。たとえば、ネットワーク２００としてインターネットを用い、外部の記憶装置３００として、インターネットに接続されたデータサーバを用いた場合、このデータサーバ上での退避対象ファイルのＵＲＬアドレスを管理情報として用いるようにすればよい。上述の例の場合、退避処理により、退避対象ファイルＦ１，Ｆ２，Ｆ３は、外部の記憶装置３００内の所定の退避場所にコピーされることになるので、この退避場所を示すＵＲＬアドレスを管理情報として作成すればよい。なお、実用上は、この管理情報には、ユーザ甲のログオフ手続で作成された管理情報であることを示す情報を含ませておくのが好ましい。

退避処理部１６０で実行される第５の処理は、作成された管理情報を外部の記憶場所に保存する管理情報保存処理である。図１に示す例では、管理情報を保存するための外部の記憶場所として、携帯可能情報記録媒体４００（具体的にはＩＣカード）を用意している。したがって、管理情報は、この携帯可能情報記録媒体４００内に保存されることになる。ログオフ手続を完了したユーザ甲は、最後に、この携帯可能情報記録媒体４００を、情報処理装置１００から取り外して携帯する。具体的には、情報処理装置１００としてのパソコンに接続されたリーダライタ装置から、携帯可能情報記録媒体４００としてのＩＣカードをエジェクトして取り出す作業を行うことになる。

以上の各処理により、ユーザ甲のログオフ手続は完了である。このようなログオフ手続を経た結果、ユーザ甲がログオン中に作業したデータファイルＦ１，Ｆ２，Ｆ３は、データ格納部１１０内から削除された状態になっている。したがって、この後、第２のユーザ乙が情報処理装置１００に対するログオン手続を行ったとしても、ユーザ乙は、ユーザ甲が作業したデータファイルＦ１，Ｆ２，Ｆ３にアクセスすることはできない。たとえユーザ乙が、管理者権限をもつ特別なユーザであっても、あるいは、不正な手段でアクセスを行ったとしても、そもそもデータファイルＦ１，Ｆ２，Ｆ３は、データ格納部１１０内には存在しないのであるから、物理的にアクセスすることはできない状態になっている。

もちろん、厳密な意味でアクセス不能にするためには、上述したとおり、データ格納部１１０内の実際のデータ記録領域に別なデータを上書きすることによりデータファイル自身を完全に削除する方法を採るのが好ましい。なお、ユーザ甲がログオフした時点で、メモリ１３０内にデータが展開されたままになっていたとしても、通常、当該データに対する作業を実行したアプリケーションプログラムが終了された時点で、当該データに対する通常の方法によるアクセスは不可能になるので、後にログオンした別なユーザ乙が、メモリ１３０内に残っていたデータファイルにアクセスすることは困難である。ただ、より高度なセキュリティを確保する必要がある場合には、退避処理部１６０が、データ格納部１１０内の退避対象ファイルに対して削除処理を実行する際に、メモリ１３０に展開されている退避対象ファイルに対しても削除する処理を行うようにすればよい。図示の例の場合、メモリ１３０上に展開されているデータファイルＦ２に対する削除処理が併せて行われることになる。具体的には、メモリ１３０を構成するＲＡＭ領域に、ランダムなデータを上書きする作業を実行すればよい。

もちろん、この第２のユーザ乙がログオフ手続を行う際にも、全く同様の手

順が実行される。すなわち、ユーザ乙の作業によりデータ格納部１１０内に作成された退避対象ファイルは、退避処理部１６０により、外部の記憶装置３００内の所定のアドレス場所にコピーされた後、データ格納部１１０内のオリジナルファイルは削除されることになる。このとき、復元に必要な管理情報が作成されることになるが、この管理情報は、ユーザ乙用の携帯可能情報記録媒体４００（ＩＣカード）に保存されることになる。

このように、ここに示す実施形態では、情報処理装置１００を共用する各ユーザは、それぞれ固有の携帯可能情報記録媒体４００（ＩＣカード）を所持しており、情報処理装置１００に対するログオン手続を行う前に、この携帯可能情報記録媒体４００を情報処理装置１００に接続した状態とし（リーダライタ装置にＩＣカードを挿入した状態とし）、ログオフ手続を完了した際には、この携帯可能情報記録媒体４００を情報処理装置１００から取り外した状態とする（リーダライタ装置からＩＣカードをエジェクトした状態とする）。

結局、本発明では、特定のユーザがログオン中に作業したデータファイルを、当該特定のユーザのログオフ手続によって、情報処理装置１００内から削除してしまうことができるため、同一の情報処理装置１００を複数のユーザで共用する場合であっても、別のユーザが作業したファイルへのアクセスは、どのようなアクセス権限をもったユーザであっても不可能になる。このため、個々のユーザが作成したデータについて、十分なセキュリティを確保することが可能になる。

もっとも、各ユーザが、再度ログオン手続を行い、情報処理装置１００を利用して、過去に作業したデータファイルの内容を閲覧したり、更新したりする際には、退避したデータファイルをデータ格納部１１０へ復元する処理を行う必要がある。たとえば、上述の例において、第２のユーザ乙がログオフ手続を行った後、再び第１のユーザ甲がログオン手続を行った場合を考えよう。この場合、退避対象ファイルＦ１，Ｆ２，Ｆ３を、外部の記憶装置３００からデー

タ格納部１１０へと復元する処理を行う必要がある。このような復元処理を行う構成要素が、復元処理部１７０である。すなわち、復元処理部１７０は、特定のユーザがログオン手続を実行した後、携帯可能情報記録媒体４００内の管理情報を参照することにより、外部の記憶装置３００に退避されている退避対象ファイルをデータ格納部１１０内にコピーして復元する復元処理を実行する。

上述したとおり、ここに示す実施形態では、個々のユーザは、それぞれ固有の携帯可能情報記録媒体４００（ＩＣカード）を所持しており、情報処理装置１００に対するログオン手続を行う前に、この携帯可能情報記録媒体４００を情報処理装置１００に接続した状態にする。たとえば、ユーザ甲が情報処理装置１００に対してログオン手続を行う際には、所持していたＩＣカードをリーダライタ装置に挿入する作業を行うことになる。ユーザ管理部１４０は、ユーザ甲からのログイン手続を認識すると、その旨を復元処理部１７０に報告し、復元処理部１７０による復元処理の実行を促す。復元処理部１７０は、携帯可能情報記録媒体４００（ユーザ甲が挿入したＩＣカード）内の管理情報を参照することにより、前回のログオフ時に退避させられた退避対象ファイルＦ１，Ｆ２，Ｆ３の退避場所アドレス（外部の記憶装置３００内の所定アドレス）を認識し、これらのファイルをデータ格納部１１０内にコピーして復元する処理を実行する。

このような復元処理が実行されれば、データファイルＦ１，Ｆ２，Ｆ３は、再びデータ格納部１１０内に格納された状態となるので、ユーザ甲は、必要に応じて、これらのデータファイルをメモリ１３０上に展開させた上で、プログラム実行部１５０による更新処理を実行することができる。もちろん、データ甲が再びログオフ手続を行えば、データファイルＦ１，Ｆ２，Ｆ３は、再び外部の記憶装置３００へと退避させられ、データ格納部１１０内からは削除されることになる。

実用上は、退避処理部１６０による退避処理は、ユーザがログオフ手続を行

ったときに自動的に行われるようにし、復元処理部１７０による復元処理は、ユーザがログオン手続を行ったときに自動的に行われるようにしておくのが好ましい。そうすれば、退避処理や復元処理は、ユーザが何ら意識しない状態で行われることになり、本発明の特徴となる退避処理部１６０や復元処理部１７０の動作は、ユーザの関知しない裏の動作ということになる。本発明の特徴は、パソコンなどの既存の情報処理装置に、退避処理部１６０および復元処理部１７０を付加した点にあるが、少なくとも一般のユーザから見れば、本発明を適用したパソコンの操作性は、既存のパソコンと何ら変わることはない。

なお、外部の記憶装置３００内からデータファイルの復元を行った場合、外部の記憶装置３００内の復元対象となったデータファイルは削除してもよいし、そのまま残しておいてもかまわない。外部の記憶装置３００の記憶容量をできるだけ節約したい場合には、復元処理部１７０による復元処理が行われたデータファイルについては、外部の記憶装置３００内から削除する処理を行えばよい。あるいは、復元処理が行われた後も、外部の記憶装置３００内のデータファイルをそのまま残しておき、次回、同じファイル名のデータファイルについて再度の退避処理を行う際に、前回との差分データのみをコピーするような方法を採ることも可能である。

＜＜＜　§３．いくつかの実用的な工夫　＞＞＞

上述の§２では、本発明の基本的な実施形態を説明した。ここでは、本発明を実施する上で、より実用的ないくつかの工夫を述べる。

(1)　退避対象ファイルの選択

上述した基本的な実施形態では、特定のユーザ甲がログオフ手続を実行したときに、データ格納部１１０に格納されているデータファイルのうち、特定のユーザ甲の作業に基づいて作成もしくは更新されたデータファイルの全部を退避対象ファイルとして認識するようにしていたが、全部ではなく所定の一部を選択して、退避対象ファイルとして認識するようにしてもかまわない。これは、

通常、すべてのデータファイルについて等しくセキュリティを確保する必要があるとは限らないからである。

ユーザの作業対象となったデータファイルのうちの一部のみを退避対象ファイルとするには、予め退避対象ファイルとして選択するための基準を定めておけばよい。たとえば、予め所定のフォルダを退避対象フォルダとして定めておき、退避処理部１６０が退避対象認識処理を行う際に、この退避対象フォルダ内に格納されているデータファイルを、退避対象ファイルとして認識するようにすればよい。

図２は、データ格納部１１０内に格納されたデータファイルの階層構造を示すウインドウ表示の一例を示す図である。図示の例では、左側のウインドウＷ１に、データ格納部１１０内の階層構造の全体像が示されており、右側のウインドウＷ２には、左側のウインドウＷ１上で選択された特定のフォルダＢ（図では、ハッチングにより選択状態を示している）の内容が示されている。この例では、データ格納部１１０全体が「Ｃ」なるボリュームで示されており、その直下に、フォルダＡ，Ｂ，Ｃなる３つのフォルダが作成されている。そして、フォルダＡにはファイルＦ０が格納され、フォルダＢにはファイルＦ１，Ｆ２，Ｆ３が格納され、フォルダＣにはファイルＦ４，Ｆ５が格納されている。

ここで、たとえば、フォルダＡに格納されているファイルＦ０が、ＯＳに関連して利用されるデータファイルであるとし、他のユーザにアクセスされても、セキュリティ上は問題がないものとしよう。また、フォルダＣに格納されているファイルＦ４，Ｆ５は、ユーザ甲が所定のアプリケーションプログラムで作成したデータファイルであるが、これらのファイルも、その性質上、セキュリティ上の問題がないものとしよう。この場合、セキュリティ上、問題が生じるファイルは、フォルダＢに格納されているファイルＦ１，Ｆ２，Ｆ３だけということになる。

このような場合は、予め、フォルダＢを退避対象フォルダと定める設定を行

っておけばよい。そうすれば、退避処理部１６０が、退避対象認識処理を実行する際に、退避対象フォルダＢ内に格納されているファイルＦ１，Ｆ２，Ｆ３を退避対象ファイルと認識することができる。その結果、図３に示すような退避処理が実行されることになる。図３(a) は退避処理前のデータ格納部１１０の状態を示しており、図３(b) は退避処理後のデータ格納部１１０および外部の記憶装置３００の状態を示している。図示のとおり、退避処理により、データ格納部１１０内のフォルダＢは、そのまま外部の記憶装置３００へとコピーされ、データ格納部１１０内からは削除されている。結局、データ格納部１１０には、フォルダＡ，Ｃのみが残っている。このフォルダＡ，Ｃ内のファイルＦ０，Ｆ４，Ｆ５については、他のユーザによるアクセスを受ける可能性があるが、上述したとおり、これらのファイルはセキュリティ上は問題がないファイルである。

ネットワーク２００を介して外部の記憶装置３００へファイルを退避する処理は、情報処理装置１００にそれなりの作業負荷を与えることになる。また、後に行われる復元処理も、同様の作業負荷を与える。したがって、実用上は、セキュリティの確保が必要なファイルと、そうでないファイルとを区分けし、前者のファイルのみを退避対象ファイルとして取り扱うようにするのが好ましい。上述の例のように、予め所定のフォルダを退避対象フォルダとして定めておく方法を採れば、ユーザ自身の判断で退避対象ファイルの取捨選択を行うことができるので便利である。上述の例の場合、ユーザは、セキュリティの確保が必要なファイルをフォルダＢに入れ、それ以外のファイルをフォルダＣに入れて区別すればよい。

もちろん、退避対象ファイルの取捨選択を行う方法は、退避対象フォルダを定めておく方法に限定されるものではない。たとえば、予め定められた所定の拡張子がファイル名に付されているデータファイルを、退避対象ファイルとして認識するような方法を採ることも可能である。一般的なＯＳでは、個々のフ

ァイルのファイル名に、当該ファイルのフォーマットや当該ファイルを作成したアプリケーションプログラムを特定するための拡張子を付加する取り扱いが行われている。たとえば.「ABC.txt」なるファイル名における「txt」は、当該ファイルが単純なテキストファイルであることを示す拡張子である。そこで、ユーザが、たとえば、ある特定のアプリケーションプログラムで作成したファイルを退避対象ファイルにしたいと考えた場合は、当該アプリケーションプログラムで作成したファイルに固有の拡張子をファイル名にもつファイルを、退避対象ファイルとして認識するような条件設定を行っておけば、退避処理部１６０によって、当該条件設定に基づく退避対象ファイルの取捨選択を自動的に実行することが可能になる。

(2) 必要に応じた復元処理

上述した基本的な実施形態では、ユーザ甲がログオン手続を実行したときに、前回退避したファイルＦ１，Ｆ２，Ｆ３のすべてを直ちにデータ格納部１１０内に復元する例を述べたが、復元処理は必ずしもすべての退避対象ファイルに対して実行する必要はなく、必要に応じて行えば足りる。たとえば、ユーザ甲のログオフ時に、図３に示す例のように、フォルダＢ内に格納されていた退避対象ファイルＦ１，Ｆ２，Ｆ３を、フォルダＢごと外部の記憶装置３００へ退避した場合を考えよう。この場合、このユーザ甲が、再度ログオンする際に、退避対象ファイルＦ１，Ｆ２，Ｆ３を、フォルダＢごとそっくりデータ格納部１１０内にコピーして復元すれば、前回のログオン時と同等の環境が復元されたことになる。しかしながら、ネットワーク２００を介した復元処理は、情報処理装置１００に作業負荷を加える要因になり、復元対象となるデータ容量が大きいと、復元処理時に、情報処理装置１００の応答性が低下するなどの弊害を生じる可能性がある。

ここで、もし、再度ログオンしたユーザ甲が、ファイルＦ２に対して何らかの更新処理を実行した後にログオフしたとすると、実際に復元する必要があっ

たファイルはファイルＦ２のみであり、ファイルＦ１，Ｆ３の復元処理は無駄ということになる。この場合、ユーザ甲の作業対象となるファイルＦ２のみを復元すれば足りる。しかしながら、ファイルＦ１，Ｆ２，Ｆ３の復元を全く行わない状態では、そもそもデータ格納部１１０内に、ファイルＦ１，Ｆ２，Ｆ３が存在していないので、ファイルリスト上にも、ファイルＦ１，Ｆ２，Ｆ３の存在が示されないことになり、ユーザ甲は、作業対象としてファイルＦ２を指定することすらできない。すなわち、図３(b) に示すような状態のままでは、データ格納部１１０内には、フォルダＡ，Ｃのみしか存在していないので、図２に示すようなファイルリスト表示を行ったとしても、フォルダＢや、その中に格納されているファイルＦ１，Ｆ２，Ｆ３が表示されることはない。

このような問題を解決するためには、復元処理部１７０に、二段階の復元処理機能をもたせておくようにすればよい。すなわち、第１段階の復元処理機能は、データファイルの保存時の階層構造を復元する予備復元処理であり、第２段階の復元処理機能は、予備復元処理によって復元された階層構造内から選択された特定のデータファイルを実際に復元する本復元処理である。

図４は、この二段階の復元処理機能の概念を説明する図である。まず、第１段階の予備復元処理では、データファイルの保存時の階層構造のみが復元される。すなわち、図４(a) に示すように、退避対象となったフォルダＢの階層構造のみの復元が行われる。図では、便宜上、階層構造のみの復元が行われたフォルダやファイルを破線のブロックで示してある。この図４(a) に示す予備復元処理の段階では、ファイルＦ１，Ｆ２，Ｆ３の実体データの復元は行われていない。しかしながら、フォルダＢの中にファイルＦ１，Ｆ２，Ｆ３が格納されている、という階層構造（フォルダ名やファイル名も含めた階層構造）についての復元は行われているので、図２に示すようなファイルリスト表示を行った場合、フォルダＢの存在や、その中にファイルＦ１，Ｆ２，Ｆ３が格納されているという階層構造を表示させることは可能になる。

結局、予備復元処理では、ファイルＦ１，Ｆ２，Ｆ３の実体データをデータ格納部１１０にコピーする必要はなく、「フォルダＢ」なる名前のフォルダの中に、「ファイルＦ１」なる名前のファイルと、「ファイルＦ２」なる名前のファイルと、「ファイルＦ３」なる名前のファイルと、が格納されている、という階層構造を示す情報のみをデータ格納部１１０内に復元すればよいので、復元すべきデータ容量は大幅に低減される。なお、図２のウインドウＷ２に示すように、各ファイルのサイズや修正日時といった書誌情報も表示させる必要がある場合には、この書誌情報も併せて復元する必要があるが、それでも復元すべきデータ容量は大幅に低減される。

このように、まず第１段階の復元処理として、予備復元処理を実行しておけば、ユーザには、とりあえず、図２に示すようなファイルリストの提示を行うことができるので、データ格納部１１０内に格納されているファイル構造が、あたかも前回のログオフ直前の状態と同等であるかのように見せることができる。実際、ユーザは、図２に示すようなファイルリストの表示を見て、データ格納部１１０内には、３つのフォルダＡ，Ｂ，Ｃが格納されている状態を確認することができ、フォルダＢの中には、ファイルＦ１，Ｆ２，Ｆ３が格納されている状態を確認することができる。

もっとも、この図２に示すようなファイルリスト表示は、パソコンなどの情報処理装置１００に備わっているＯＳの標準機能では行うことができない。すなわち、データ格納部１１０内には、実際にフォルダＢ内のファイルの復元が行われているわけではなく、その階層構造を示すデータのみが所定のフォーマットで書き込まれているにすぎないので、この所定のフォーマットを解釈して、図２に示すようなウインドウ上に階層構造をファイルリストとして表示する機能を果たす専用のアプリケーションプログラムが必要になる。したがって、復元処理部１７０は、このような専用のアプリケーションプログラムを含んだ構成要素ということになる。

さて、図２に示すウインドウＷ２上で、ユーザがファイルＦ２のアイコンをダブルクリックするなどして、ファイルＦ２をメモリ１３０上に展開する指示を与えたとしよう（あるいは、所定のアプリケーションプログラムから、ファイルＦ２を開く指示を与えても同様である）。この場合、図４(a) に示すように、ファイルＦ２の実体は、データ格納部１１０にはまだ存在しないので、ファイルＦ２を直ちにメモリ１３０上に展開する処理を行うことはできない。その代わりに、復元処理部１７０が、ファイルＦ２に対する本復元処理を実行する。すなわち、携帯可能情報記録媒体４００内の管理情報を参照して、ファイルＦ２の退避場所アドレスを認識し、ファイルＦ２の実体となるデータファイルを実際にデータ格納部１１０内へと復元する処理が実行される。図４(b) は、このような本復元処理が実行された後のデータ格納部１１０内の状態を示す図である。破線で示すファイルＦ１，Ｆ３の実体は依然として復元されていない状態であるが、実線で示すファイルＦ２は、その実体がデータ格納部１１０内に復元されることになるので、これをメモリ１３０上に展開することが可能になる。

もっとも、ユーザから見れば、単に、所望のファイルＦ２を所定のアプリケーションプログラムで開く作業を行っただけであり、上述した本復元処理が行われたことは、ユーザの意識する事項ではない。別言すれば、ユーザから見た操作性は、従来の一般的なパソコンに対する操作性とほぼ同じである。ここで、このユーザが、プログラム実行部１５０に対して所定の操作を行うことにより、メモリ１３０上に展開されているデータファイルＦ２に対して、何らかの更新処理を行った後、これを保存する操作を行えば、更新後のデータファイルＦ２は、データ格納部１１０内のデータファイルＦ２に上書き保存されることになる。そして、このユーザが、ここでログオフ手続を行ったとすると、退避処理部１６０により、データ格納部１１０内に実在するデータファイルＦ２が退避対象ファイルとして認識され、退避処理が実行される。そして、携帯可能情報記録媒体４００内の管理情報のうち、データファイルＦ２の退避場所アドレス

が書き換えられることになる。

このような運用を行えば、実際に復元する必要があったデータファイルＦ２に対してのみ本復元処理が実行されることになり、ログオフ時には、当該データファイルＦ２に対してのみ退避処理が実行されることになるので、全データファイルを一括して復元し、一括して退避する方法に比べて、より効率的な運用が可能になる。

(3) 退避対象ファイルの分割処理および暗号化処理

本発明による退避処理が行われると、情報処理装置１００内には退避対象ファイルは残っていないので、情報処理装置１００に関する限り、十分なセキュリティが確保されることになる。しかしながら、退避対象ファイルは、外部の記憶装置３００に格納されているため、この外部の記憶装置３００に対するアクセスにより、セキュリティが破られるおそれがある。もっとも、実用上は、ネットワーク２００としてインターネットを用いるようにすれば、外部の記憶装置３００は、インターネットに接続された任意の記憶装置によって構成することができるため、特定の退避対象ファイルの退避場所を知ることは、携帯可能情報記録媒体４００内の管理情報を参照しない限り、事実上不可能である。したがって、個々のユーザが、それぞれ所持する携帯可能情報記録媒体４００をしっかりと管理していれば、退避対象ファイルの退避場所が外部に漏えいする危険性は低い。特に、携帯可能情報記録媒体４００としてＩＣカードを利用すれば、内部に保存した管理情報が不正な手段で外部に読み出される可能性は極めて低い。

しかしながら、外部の記憶装置３００は、インターネットに接続された環境にあるため、何者かによる直接攻撃の対象になるおそれがあり、退避対象ファイルが、そのまま不正な手段で外部へ読み出される可能性がある。このような問題に対処するためには、退避対象ファイルに対して分割処理を施したり、暗号化処理を施したりするのが好ましい。以下、このような対策を具体例に即し

て説明する。

図５は、退避対象ファイルに対する分割処理の概念を示す図である。ここでは、退避対象となったファイルＦ２に対して分割処理を行う一例が示されている。すなわち、この例では、データ格納部１１０内のファイルＦ２を退避する際に（外部の記憶装置にコピーする際に）、退避処理部１６０によって、ファイルＦ２を３つの分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃに分割する処理が実行される。そして、この３つの分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃが、ネットワーク２００を介して、それぞれ異なる外部の記憶装置に退避される。

図６は、３つの分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃを、それぞれ異なる記憶装置に退避するために、ネットワーク２００に３つの異なる記憶装置を接続した変形例を示すブロック図である。図１に示す基本的な実施形態と、この図６に示す変形例との相違は、後者では、退避場所として第１の記憶装置３１０，第２の記憶装置３２０，第３の記憶装置３３０が用意されている点と、退避処理部１６０が分割処理を行う点と、復元処理部１７０が分割ファイルを合成して復元処理を行う点である。

そこで、以下、図６を参照しながら、退避処理部１６０による退避処理と、復元処理部１７０による復元処理とが、どのように行われるかを説明する。ここでは、便宜上、ログオン中のユーザ甲がログオフ手続を行った時点で、データ格納部１１０内には、図示のとおり、３つのデータファイルＦ１，Ｆ２，Ｆ３が格納されており、そのうちデータファイルＦ２が退避対象ファイルとなっていたという前提で、以下の説明を行うことにする。

ユーザ甲がログオフ手続を行うと、既に述べたとおり、退避処理部１６０によって、５つの処理が実行される。すなわち、この例の場合、まず、退避対象認識処理により、データ格納部１１０内のデータファイルＦ２が退避対象ファイルとして認識される。続いて、退避処理が行われるが、このとき、データファイルＦ２に対する分割処理が行われ、データファイルＦ２は複数の分割ファ

イルに分割された状態で、外部の記憶装置へとコピーされることになる。具体的には、図５に示す例では、ファイルＦ２は、３つの分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃに分割され、それぞれ第１の記憶装置３１０，第２の記憶装置３２０，第３の記憶装置３３０へとコピーされることになる。

この退避処理が完了したら、データ格納部１１０内のデータファイルＦ２を削除する削除処理が行われる。そして、管理情報作成処理が行われ、作成された管理情報を携帯可能情報記録媒体４００に保存する管理情報保存処理が行われる。この変形例の場合、データファイルＦ２について作成される管理情報について留意すべき点が２つある。

第１点は、ファイルＦ２の退避場所を示すアドレスとして、個々の分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃのそれぞれの退避場所となった３ヶ所のアドレスを、管理情報に含ませておく点である。具体的には、第１の記憶装置３１０内の分割ファイルＦ２ａの格納先を示すＵＲＬアドレスと、第２の記憶装置３２０内の分割ファイルＦ２ｂの格納先を示すＵＲＬアドレスと、第３の記憶装置３３０内の分割ファイルＦ２ｃの格納先を示すＵＲＬアドレスと、が管理情報として用意されることになる。そもそも本発明における管理情報とは、外部の記憶装置に退避された退避対象ファイルをデータ格納部１１０内にコピーして復元するために必要な情報であるから、退避対象ファイルＦ２が３つに分割され、それぞれ異なる場所に退避されたのであれば、個々の分割ファイルの退避場所アドレスを管理情報として用意するのは当然である。

第２点は、退避対象ファイルＦ２に対して施した分割処理の方法を示す情報を、管理情報に含ませておく点である。たとえば、図５に示す分割処理は、「退避対象ファイルＦ２を３つに等分割し、先頭から順に、分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃとする」という分割方法によって行われることになるので、当該分割方法を示す情報を管理情報に含ませておくようにする。そうすれば、後に復元処理部１７０による復元処理を行う際に、管理情報内の分割方法を示す

情報を参照することにより、分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃを合成して、元のデータファイルＦ２を復元することが可能になる。

結局、この分割処理を施す変形例では、退避処理部１６０は、退避処理を実行する際に、退避対象ファイルを所定の分割方法に基づいて複数の分割ファイルに分割し、個々の分割ファイルをそれぞれ異なる複数の記憶装置に退避させる処理を実行し、実施した分割方法を示す情報を含む管理情報を作成するようにし、復元処理部１７０は、この管理情報に含まれている分割方法を示す情報に基づいて、退避対象ファイルの復元を行うようにすればよい。

この変形例のメリットは、外部の記憶装置へ退避される退避対象ファイルが、そのままの形ではなく、複数の分割ファイルとして、ばらばらに格納される点にある。たとえば、上述の例の場合、データファイルＦ２は、３つの分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃに分割された上、３ヶ所に分散して格納されることになるので、万一、いずれかの分割ファイルが不正な手段でアクセスされたとしても、もとのデータファイルＦ２自身が直ちに露見することは防げる。

この変形例において、セキュリティの効果をできるだけ高めるには、より複雑な分割方法を採るようにすればよい。たとえば、図５に示す例では、元のファイルＦ２を３等分するという単純な分割方法を採用しているため、万一、分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃのすべてが不正な手段によって入手されてしまうと、これらをこの順に合成することにより、元のファイルＦ２を復元することが可能になる。これに対して、たとえば、同じ３つのファイルに分割する方法でも、元のファイルＦ２を構成するバイト列の先頭から、１，４，７，１０，…バイト目というように３バイト周期で１バイトずつを抜き出すことにより第１の分割ファイルＦ２ａを作成し、２，５，８，１１，…バイト目というように３バイト周期で１バイトずつを抜き出すことにより第２の分割ファイルＦ２ｂを作成し、３，６，９，１２，…バイト目というように３バイト周期で１バイトずつを抜き出すことにより第３の分割ファイルＦ２ｃを作成する、

という分割方法を採った場合、このような分割方法が行われたことを知らない者にとっては、３つの分割ファイルＦ２ａ，Ｆ２ｂ，Ｆ２ｃを入手できたとしても、元のファイルＦ２を復元することは困難になる。

実際には、このような分割方法の原理は無限に存在し、また、同じ原理に基づく分割方法でも、パラメータ値を種々変えることにより、実質的には異なる分割方法になる。したがって、退避処理部１６０内に予め複数通りの分割方法を定義しておき、更に、パラメータをランダムに設定するようにすれば、実質的に無限通りの分割方法の中の１つを選択することができるので、退避対象ファイルごとに、それぞれ異なる分割方法を適用して退避させることが可能になる。

また、図６では、外部の記憶装置として、３つの記憶装置３１０，３２０，３３０を用いる例を示したが、ネットワーク２００としてインターネットを用いるようにすれば、これら外部の記憶装置は、理論上無限に設置することができる。したがって、これら外部の記憶装置のそれぞれが、不正な手段でアクセスされる可能性があったとしても、特定の退避対象ファイルが、どのような分割方法でいくつに分割され、その結果として生成された個々の分割ファイルがどの記憶装置のどのアドレスに格納されたか、という事項を示す管理情報（これは、ユーザが所持する携帯可能情報記録媒体４００内にのみ保存されている）がない限り、第三者が退避対象ファイルを復元することは不可能である。

このような分割処理と同様にセキュリティ確保に有効な手段は、暗号化処理である。すなわち、退避処理部１６０が、退避処理を実行する際に、退避対象ファイルを所定の暗号化方法に基づいて暗号化した上で外部の記憶装置に退避させる処理を実行し、当該暗号化方法を示す情報を含む管理情報を作成するようにし、復元処理部１７０が、退避対象ファイルの復元を行う際に、この管理情報に含まれている暗号化方法を示す情報に基づいて復号化処理を実行するようにすればよい。

たとえば、データファイルＦ２が退避対象である場合、このデータファイルＦ２に対して、所定の暗号化プロセスを施して、暗号化ファイルＦＦ２を生成し、この暗号化ファイルＦＦ２を外部の記憶装置へコピーして格納すればよい。このとき、どのような暗号化プロセスを施したかを示す情報（暗号化のために何らかのキーを用いた場合には、当該キーも含めた情報）を、管理情報に含めておくようにする。そうすれば、万一、外部の記憶装置に格納されている暗号化ファイルＦＦ２が不正にアクセスされたとしても、暗号解読ができない限り、セキュリティ上の支障は生じない。もちろん、正規のユーザがログオンしたときには、携帯可能情報記録媒体４００内の管理情報に含まれている暗号化方法を示す情報に基づいて、暗号化ファイルＦＦ２に対する復号化処理を行うことができるので、元のデータファイルＦ２を復元することが可能である。

もちろん、より高いセキュリティを確保するために、分割化処理と暗号化処理とを組み合わせることも可能である。たとえば、退避対象ファイルを分割して複数の分割ファイルを生成した後、個々の分割ファイルのそれぞれに対して暗号化処理を施した上で、外部の記憶装置へと退避させるようなことも可能であるし、逆に、退避対象ファイルを暗号化した上で、この暗号化されたファイルを分割して複数の分割ファイルを生成し、これらを外部の記憶装置へと退避させるようなことも可能である。

(4)　管理情報の保存場所

本発明を実施する上で、管理情報は重要な役割を果たす。すなわち、管理情報は、外部の記憶装置へ退避した退避対象ファイルを復元するために必要な情報であり、復元処理部１７０による復元処理に不可欠の情報である。その半面、この管理情報が、他のユーザの手に入ってしまうと、当該他のユーザによっても、退避対象ファイルの復元が可能になってしまうため、セキュリティ確保の観点からは、この管理情報は、情報処理装置１００の内部ではなく、外部の記憶場所に保存する必要がある。

そこで、これまで述べた実施形態では、情報処理装置１００に対して着脱自在な携帯可能情報記録媒体４００を管理情報の記憶場所とするようにし、退避処理部１６０が管理情報を保存する際には、この携帯可能情報記録媒体４００を保存場所とし、復元処理部１７０が復元処理を行う際には、この携帯可能情報記録媒体４００に保存されている管理情報を参照した復元が行われるようにしている。特に、上述した実施形態では、ＩＣカードを携帯可能情報記録媒体４００として用いる運用を行っている。具体的には、予め、個々のユーザごとにそれぞれ固有のＩＣカードを発行しておき、ログイン手続を行う際には、必ずこのＩＣカードをリーダライタ装置に挿入させるようにし、ログオフ手続を行った後は、必ずこのＩＣカードをリーダライタ装置からエジェクトして携帯させるような運用を行っている。

しかしながら、本発明を実施する上では、管理情報は必ずしもＩＣカードのような携帯可能情報記録媒体４００に保存する必要はない。すなわち、管理情報は、情報処理装置１００の外部に存在し、正規のユーザによるアクセスのみが可能となるような環境下にある記憶場所に保存できれば、必ずしも携帯可能情報記録媒体４００に保存する必要はない。具体的には、たとえば、管理情報を、ネットワーク２００を介して接続された外部のサーバ装置などに保存するようにし、保存先のＵＲＬアドレスを正規のユーザに対してのみ知らせておくような運用を採ることも可能である。この場合、ユーザは、ログオン手続時に当該ＵＲＬアドレスを入力する操作を行えばよい。復元処理部１７０は、この入力されたＵＲＬアドレスに存在する管理情報を参照することにより、必要なファイルの復元処理を行うことができる。

(5)　情報処理装置１００の具体的な構築方法

実用上、図１に示す情報処理装置１００として機能する代表的な装置はパソコンである。既に§１で述べたとおり、この図１のブロック図に示す構成要素のうち、データ格納部１１０、展開保存部１２０、メモリ１３０、ユーザ管理

部１４０、プログラム実行部１５０なる構成要素によって実現される機能は、現在市販されている一般的なパソコン（所定のＯＳが組み込まれたパソコン）に標準的に備わっている機能である。したがって、このような市販のパソコンを、本発明に係る情報処理装置１００として利用するには、このパソコンに、退避処理部１６０および復元処理部１７０としての機能を追加し、携帯可能情報記録媒体４００などの管理情報の記憶場所を準備すればよい。ここで、退避処理部１６０および復元処理部１７０としての機能は、プログラムによって実現できるので、結局、実用上は、市販の汎用パソコンに、退避処理部１６０および復元処理部１７０としての機能を果たす専用のプログラムを組み込むことにより、本発明に係るデータ格納部１１０を構成することが可能である。もちろん、この専用のプログラムは、ＣＤ－ＲＯＭなどのコンピュータ読取り可能な記録媒体に記録して配付することも可能であるし、オンラインで配付することも可能である。

このように、本発明に係る情報処理装置は、汎用パソコンに専用プログラムを組み込むことにより実現できる装置なので、企業などで本発明に係る情報処理装置を利用する場合、実用上は、複数の情報処理装置を同時に導入し、並列的に運用する形態が一般的になるものと予想される。この場合、退避対象ファイルについての復元処理は、必ずしも当該ファイルについての退避処理を行った同一の情報処理装置で行う必要はない。

たとえば、図１に示すような情報処理装置１００として機能するパソコンが、東京本社に設置されるとともに、大阪支社にも設置されたとしよう。この場合、東京本社の社員であるユーザ甲が、東京本社に設置されている情報処理装置１００（東京）にログオンし、データファイルＦ２を作成する作業を行い、ログオフする際に、当該データファイルＦ２が退避対象ファイルとして、外部の記憶装置３００へ退避されたものとしよう。この場合、このユーザ甲が、後日、再び情報処理装置１００（東京）にログオンすれば、データファイルＦ２は、

この情報処理装置１００（東京）内に復元されることになる。しかし、このユーザ甲が、大阪に出張した際に、大阪支社に設置されている情報処理装置１００（大阪）にログオンすれば、データファイルＦ２は、この情報処理装置１００（大阪）内に復元されることになる。

要するに、ユーザ甲が作成したデータファイルＦ２の退避処理に関する情報は、ユーザ甲の所持する携帯可能情報記録媒体４００内に管理情報として保存されているので、ユーザ甲は、この携帯可能情報記録媒体４００を携帯している限り、どの情報処理装置を用いても、データファイルＦ２の復元が可能になる。実際、ネットワーク２００としてインターネットを用いるようにすれば、外部の記憶装置３００に対しては、世界中のどこからでもアクセスすることが可能になるので、ユーザ甲は、ニューヨーク支社に設置された情報処理装置１００（Newyork）にログオンしてデータファイルＦ２を復元することも可能になるし、ロンドン支社に設置された情報処理装置１００（London）にログオンしてデータファイルＦ２を復元することも可能になる。このように、自分が作成したデータファイルを、どこからでも利用することができるようになる、という効果は、セキュリティを確保するという目的を達成するために生まれた本発明の副次的な効果というべきものである。

## 産業上の利用可能性

本発明は、パソコンなどの情報処理装置を、複数のユーザによって共有して利用する場合に広く利用することができる。特に、複数ユーザによって共有されている情報処理装置において、個々のユーザが作成したデータについて十分なセキュリティを確保する環境で利用するのに最適である。

# 請求の範囲

1．　データファイルを格納するためのデータ格納部（１１０）と、

前記データ格納部に格納されているデータファイルを必要に応じて展開するためのメモリ（１３０）と、

複数のユーザによる重複ログオンが行われることがないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部（１４０）と、

ログオン中のユーザの操作に基づいて、前記データ格納部（１１０）に格納されている所定のデータファイルを前記メモリ（１３０）上に展開するファイル展開処理と、前記メモリ（１３０）上に展開されている所定のデータファイルを前記データ格納部（１１０）に格納するファイル保存処理と、を実行する展開保存部（１２０）と、

ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、前記メモリ（１３０）上に新たなデータファイルを作成する処理もしくは前記メモリ（１３０）上に展開されている既存のデータファイルに対する更新処理を実行するプログラム実行部（１５０）と、

特定のユーザがログオフ手続を実行したときに、前記データ格納部（１１０）に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、前記退避対象ファイルをネットワーク（２００）を介して外部の記憶装置（３００）にコピーすることにより退避させる退避処理と、前記データ格納部（１１０）内に格納されている前記退避対象ファイルを削除する削除処理と、前記外部の記憶装置（３００）に退避された退避対象ファイルを前記データ格納部（１１０）内にコピーして復元

するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所（４００）に保存する管理情報保存処理と、を実行する退避処理部（１６０）と、

前記特定のユーザがログオン手続を実行した後、必要に応じて、前記管理情報を参照することにより、前記外部の記憶装置（３００）に退避されている退避対象ファイルを前記データ格納部（１１０）内にコピーして復元する復元処理を実行する復元処理部（１７０）と、

を備えることを特徴とする情報処理装置（１００）。

２．　請求項１に記載の情報処理装置（１００）において、

復元処理部（１７０）が、データファイルの保存時の階層構造を復元する予備復元処理と、この予備復元処理によって復元された階層構造内から選択された特定のデータファイルを復元する本復元処理と、を実行することを特徴とする情報処理装置。

３．　請求項１または２に記載の情報処理装置（１００）において、

退避処理部（１６０）が、予め定められた退避対象フォルダ内に格納されているデータファイルを、退避対象ファイルとして認識することを特徴とする情報処理装置。

４．　請求項１または２に記載の情報処理装置（１００）において、

退避処理部（１６０）が、予め定められた所定の拡張子がファイル名に付されているデータファイルを、退避対象ファイルとして認識することを特徴とする情報処理装置。

５．　請求項１～４のいずれかに記載の情報処理装置（１００）において、

退避処理部（１６０）が、管理情報保存処理を実行する際に、着脱自在な携帯可能情報記録媒体（４００）に管理情報を保存し、

復元処理部（１７０）が、復元処理を実行する際に、前記携帯可能情報記録媒体（４００）に保存されている管理情報を参照することを特徴とする情報処理装置。

６．　請求項１～５のいずれかに記載の情報処理装置（１００）において、

管理情報として、退避対象ファイルの退避先となる外部の記憶装置のアドレス情報を用いることを特徴とする情報処理装置。

７．　請求項１～６のいずれかに記載の情報処理装置（１００）において、

退避処理部（１６０）が、退避処理を実行する際に、退避対象ファイルを所定の分割方法に基づいて複数の分割ファイルに分割し、個々の分割ファイルをそれぞれ異なる複数の記憶装置（３１０，３２０，３３０）に退避させる処理を実行し、前記所定の分割方法を示す情報を含む管理情報を作成する機能を有し、

復元処理部（１７０）が、前記管理情報に含まれている前記所定の分割方法を示す情報に基づいて、退避対象ファイルの復元を行うことを特徴とする情報処理装置。

８．　請求項１～７のいずれかに記載の情報処理装置（１００）において、

退避処理部（１６０）が、退避処理を実行する際に、退避対象ファイルを所定の暗号化方法に基づいて暗号化した上で外部の記憶装置（３００）に退避させる処理を実行し、前記所定の暗号化方法を示す情報を含む管理情報を作成する機能を有し、

復元処理部（１７０）が、前記管理情報に含まれている前記所定の暗号化方

法を示す情報に基づいて復号化処理を実行し、退避対象ファイルの復元を行うことを特徴とする情報処理装置。

９．　請求項１～８のいずれかに記載の情報処理装置（１００）において、

退避処理部（１６０）が、削除処理を実行する際に、メモリに展開されている退避対象ファイルに対しても削除する処理を行うことを特徴とする情報処理装置。

１０．　請求項１～９のいずれかに記載の情報処理装置（１００）としてコンピュータを機能させるコンピュータプログラムまたは当該プログラムを記録したコンピュータ読取り可能な記録媒体。

１１．　データファイルを格納するためのデータ格納部（１１０）と、

前記データ格納部に格納されているデータファイルを必要に応じて展開するためのメモリ（１３０）と、

複数のユーザによる重複ログオンが行われることがないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部（１４０）と、

ログオン中のユーザの操作に基づいて、前記データ格納部（１１０）に格納されている所定のデータファイルを前記メモリ（１３０）上に展開するファイル展開処理と、前記メモリ（１３０）上に展開されている所定のデータファイルを前記データ格納部（１１０）に格納するファイル保存処理と、を実行する展開保存部（１２０）と、

ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、前記メモリ（１３０）上に新たなデータファイルを作成する処理も

しくは前記メモリ（１３０）上に展開されている既存のデータファイルに対する更新処理を実行するプログラム実行部（１５０）と、

を備える情報処理装置（１００）を、複数のユーザで共用する場合に、個々のユーザごとにデータのセキュリティを確保する方法であって、

特定のユーザがログオフ手続を実行したときに、前記データ格納部（１１０）に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、前記退避対象ファイルをネットワーク（２００）を介して外部の記憶装置（３００）にコピーすることにより退避させる退避処理と、前記データ格納部（１１０）内に格納されている前記退避対象ファイルを削除する削除処理と、前記外部の記憶装置（３００）に退避された退避対象ファイルを前記データ格納部（１１０）内にコピーして復元するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所（４００）に保存する管理情報保存処理と、を実行する退避処理段階と、

前記特定のユーザがログオン手続を実行した後、必要に応じて、前記管理情報を参照することにより、前記外部の記憶装置（３００）に退避されている退避対象ファイルを前記データ格納部（１１０）内にコピーして復元する復元処理を実行する復元処理段階と、

を前記情報処理装置（１００）に行わせることを特徴とする情報処理装置におけるセキュリティ確保方法。

１２．　請求項１１に記載のセキュリティ確保方法において、

復元処理段階が、データファイルの保存時の階層構造を復元する予備復元段階と、この予備復元段階によって復元された階層構造内から選択された特定のデータファイルを復元する本復元段階と、によって構成されることを特徴とす

る情報処理装置におけるセキュリティ確保方法。

１３．　請求項１１または１２に記載のセキュリティ確保方法における退避処理段階および復元処理段階をコンピュータに実行させるコンピュータプログラムまたは当該プログラムを記録したコンピュータ読取り可能な記録媒体。

# 要　約　書

情報処理装置（１００）にログオン中のユーザがログオフ手続を実行すると、退避処理部（１６０）により以下の処理が実行される。まず、データ格納部（１１０）内に残っているファイルの中から、セキュリティ確保が必要なファイルとして認識された退避対象ファイルが、ネットワーク（２００）を介して外部の記憶装置（３００）へコピーされ、データ格納部（１１０）内の元のファイルは削除される。このとき、コピー先のアドレスが管理情報として、当該ユーザの所持する携帯可能情報記録媒体（４００）に保存される。当該ユーザが、再び情報処理装置（１００）にログオンすると、復元処理部（１７０）が、携帯可能情報記録媒体（４００）内の管理情報に基づいて、外部の記憶装置（３００）へ退避されていたファイルをデータ格納部（１１０）内に復元する。同一の情報処理装置を複数のユーザで共有する場合に、十分なセキュリティを確保できる。

図１

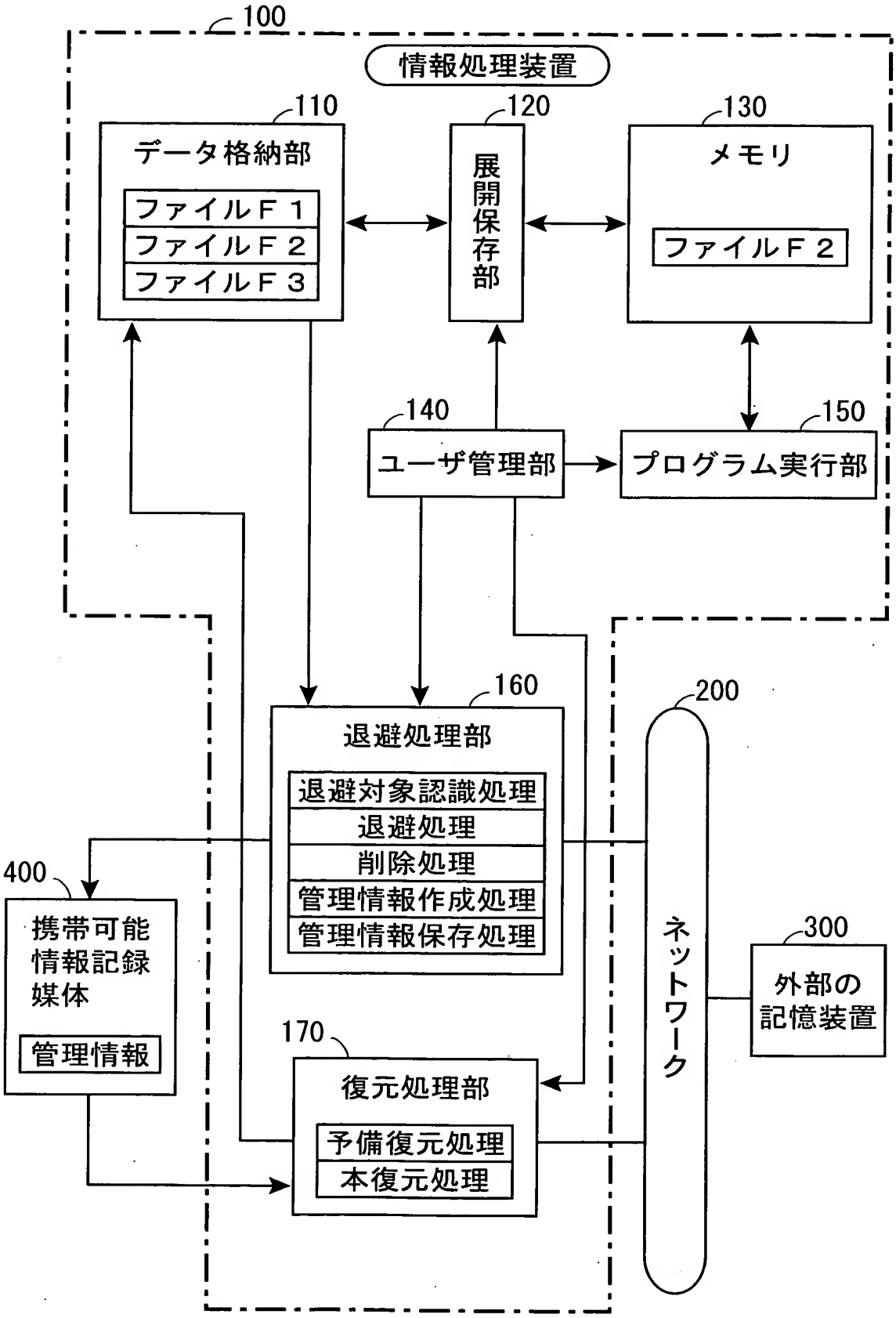

100
情報処理装置
110
データ格納部
ファイルＦ１
ファイルＦ２
ファイルＦ３
120
展開保存部
130
メモリ
ファイルＦ２
140
ユーザ管理部
150
プログラム実行部
160
退避処理部
退避対象認識処理
退避処理
削除処理
管理情報作成処理
管理情報保存処理
200
ネットワーク
300
外部の記憶装置
400
携帯可能情報記録媒体
管理情報
170
復元処理部
予備復元処理
本復元処理

図２

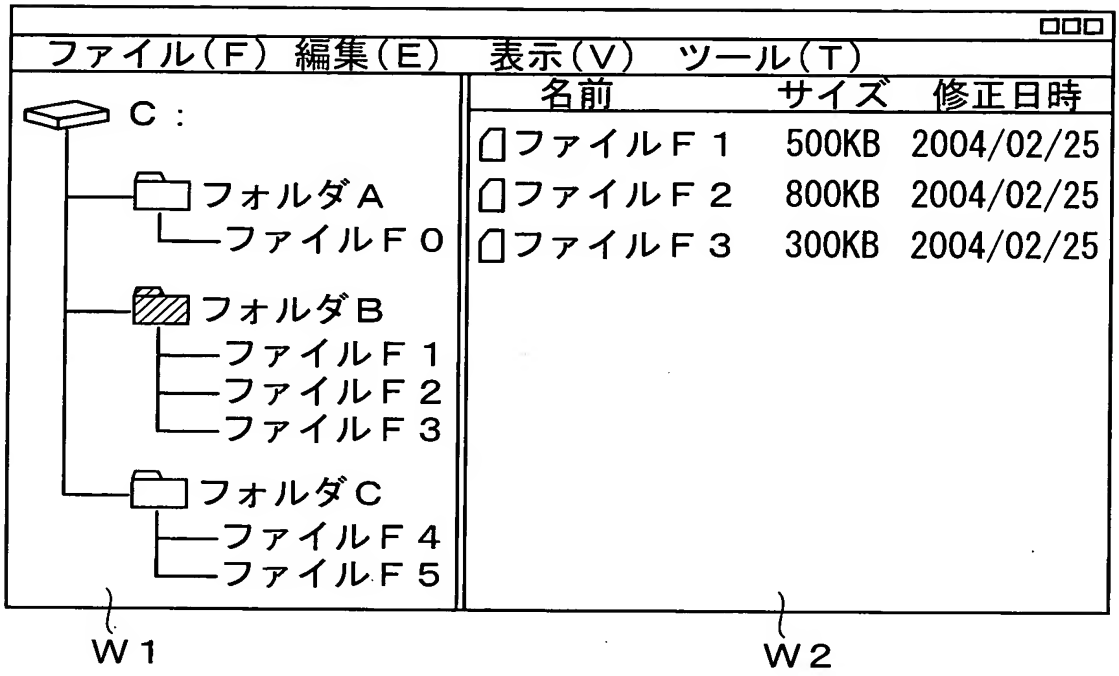

ファイル(F) 編集(E) 表示(V) ツール(T)
C：
フォルダＡ
ファイルＦ０
フォルダＢ
ファイルＦ１
ファイルＦ２
ファイルＦ３
フォルダＣ
ファイルＦ４
ファイルＦ５
名前 サイズ 修正日時
ファイルＦ１ 500KB 2004/02/25
ファイルＦ２ 800KB 2004/02/25
ファイルＦ３ 300KB 2004/02/25
Ｗ１
Ｗ２

図３

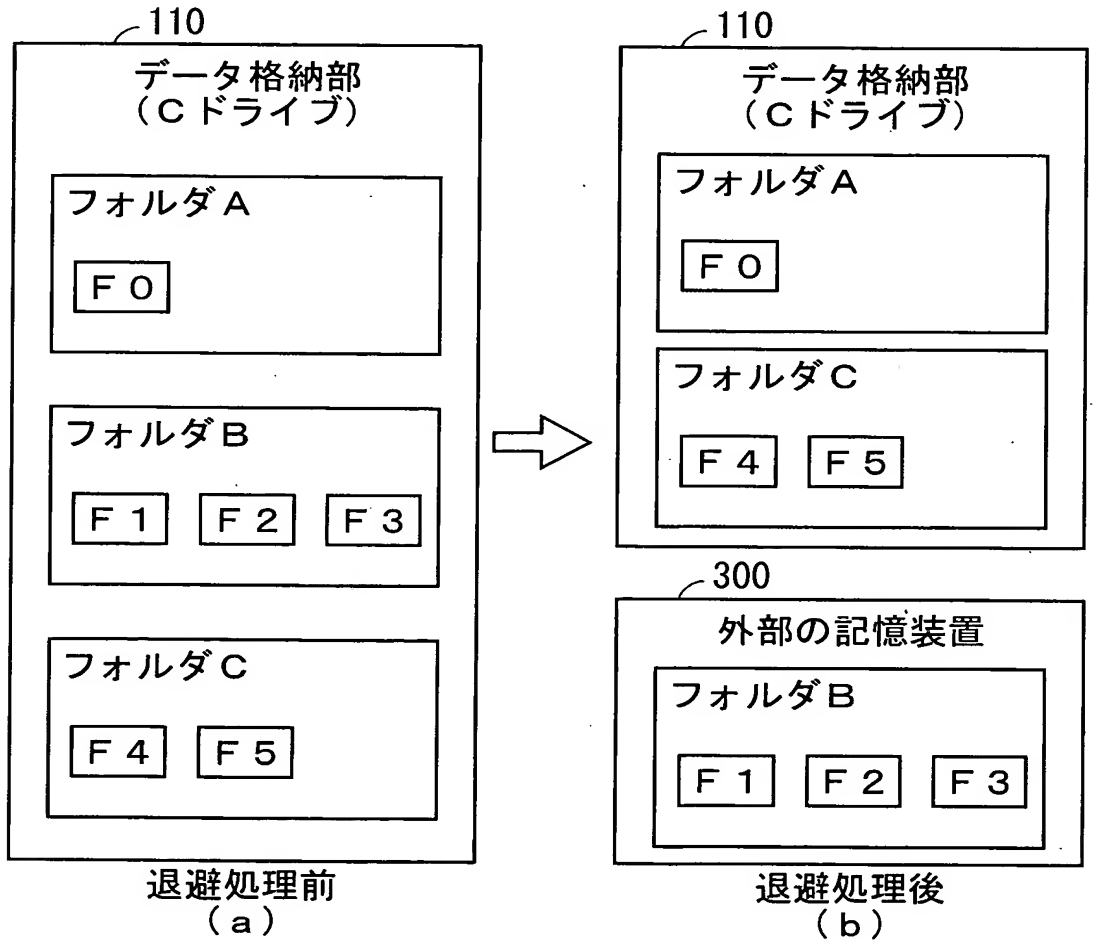

110
データ格納部
（Ｃドライブ）
フォルダＡ
Ｆ０
フォルダＢ
Ｆ１ Ｆ２ Ｆ３
フォルダＣ
Ｆ４ Ｆ５
退避処理前
（ａ）
110
データ格納部
（Ｃドライブ）
フォルダＡ
Ｆ０
フォルダＣ
Ｆ４ Ｆ５
300
外部の記憶装置
フォルダＢ
Ｆ１ Ｆ２ Ｆ３
退避処理後
（ｂ）

図４

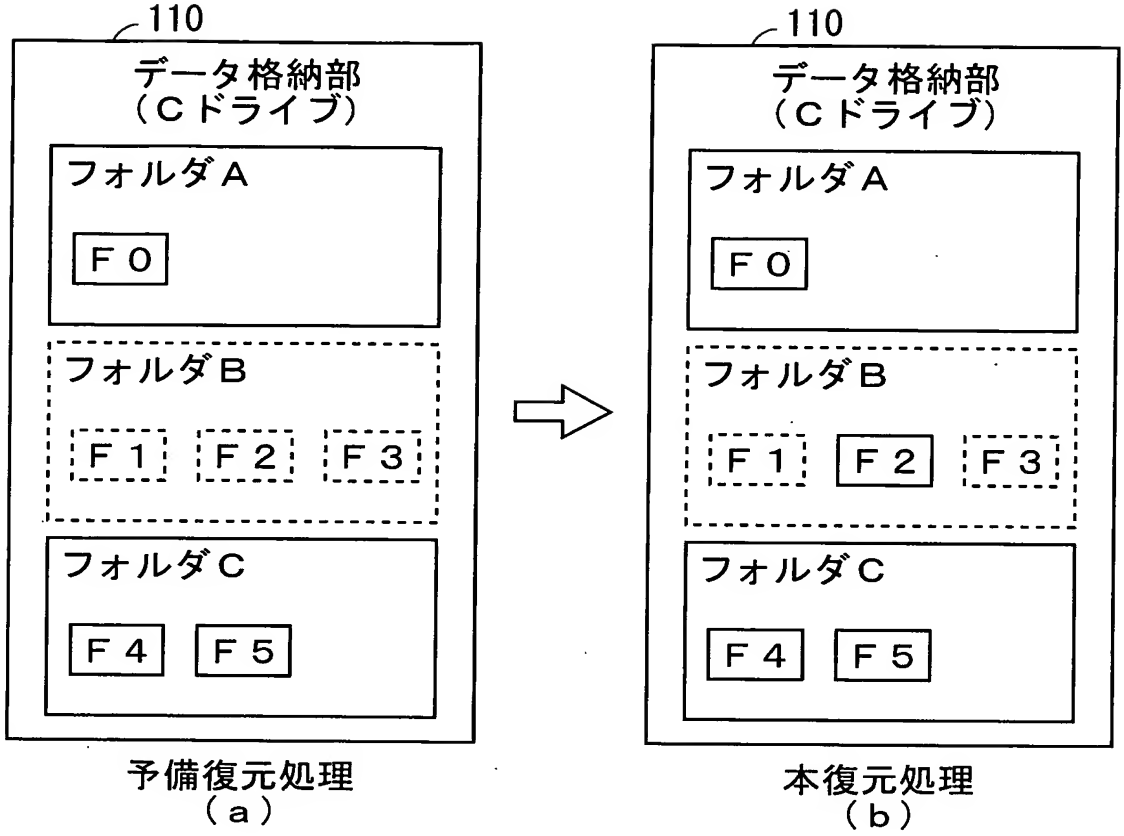

110
データ格納部
（Ｃドライブ）
フォルダＡ
Ｆ０
フォルダＢ
Ｆ１
Ｆ２
Ｆ３
フォルダＣ
Ｆ４
Ｆ５
予備復元処理
（ａ）
110
データ格納部
（Ｃドライブ）
フォルダＡ
Ｆ０
フォルダＢ
Ｆ１
Ｆ２
Ｆ３
フォルダＣ
Ｆ４
Ｆ５
本復元処理
（ｂ）

図５

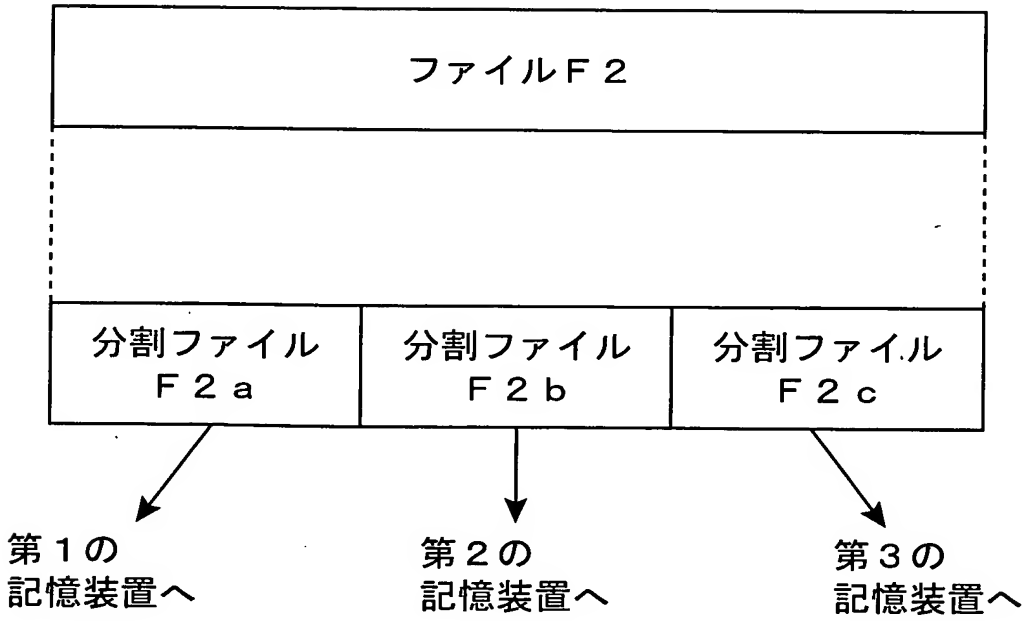
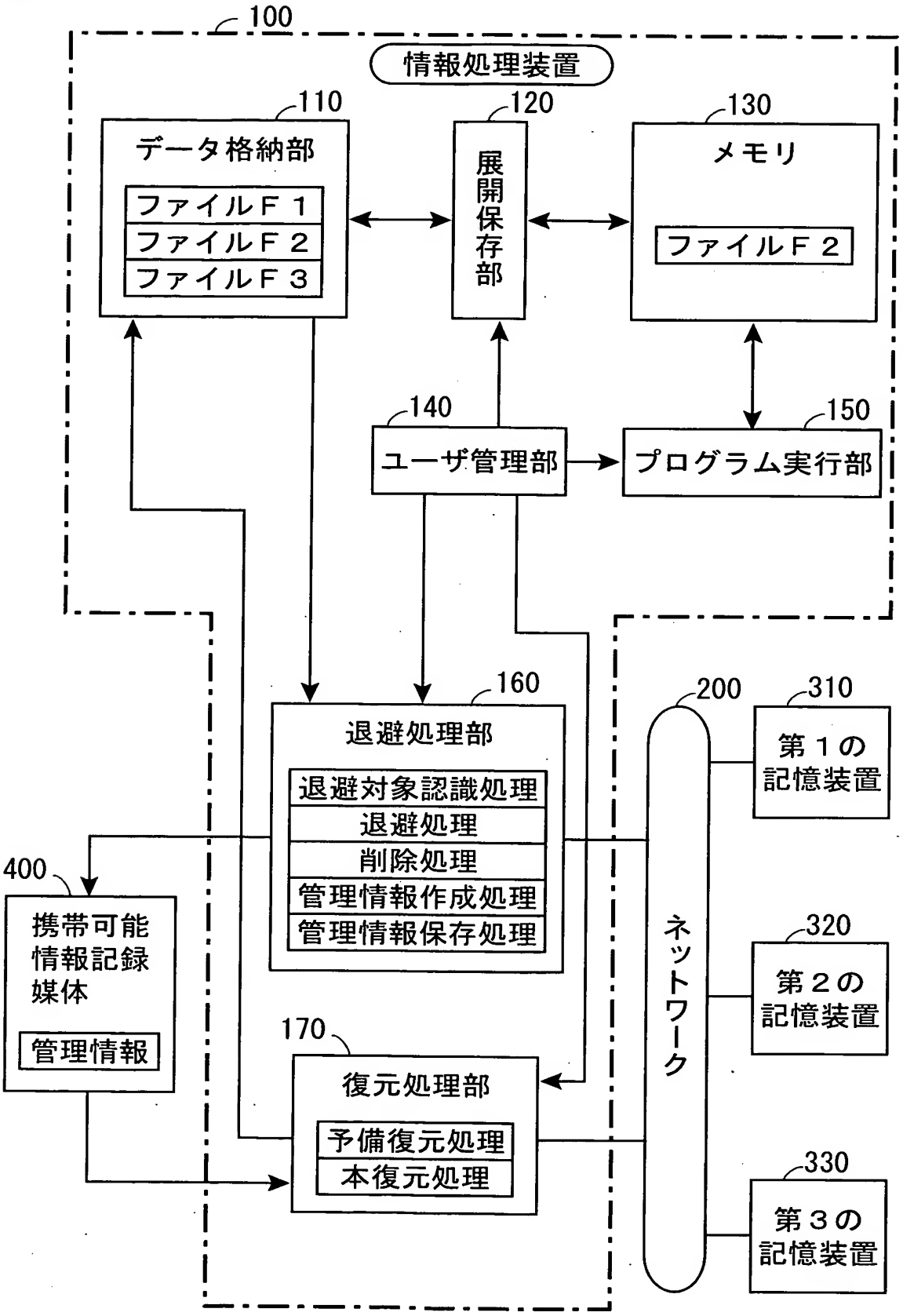

ファイルＦ２
分割ファイル
Ｆ２ａ
分割ファイル
Ｆ２ｂ
分割ファイル
Ｆ２ｃ
第１の
記憶装置へ
第２の
記憶装置へ
第３の
記憶装置へ

図６


100
情報処理装置
110
データ格納部
ファイルＦ１
ファイルＦ２
ファイルＦ３
120
展開保存部
130
メモリ
ファイルＦ２
140
ユーザ管理部
150
プログラム実行部
160
退避処理部
退避対象認識処理
退避処理
削除処理
管理情報作成処理
管理情報保存処理
170
復元処理部
予備復元処理
本復元処理
200
ネットワーク
310
第１の記憶装置
320
第２の記憶装置
330
第３の記憶装置
400
携帯可能情報記録媒体
管理情報